

AD-A081 919

ELECTRONICS ENGINEERING GROUP (1842ND) SCOTT AFB IL F/G 17/2
PACKET SWITCHING TECHNOLOGY FOR ALTERNATE CRITICAL COMMUNICATIO--ETC(U)
FEB 80 H KIN, D G WALLACE
1842EEG/EETS-TR-80-6

UNCLASSIFIED

NL

1 of 1
AD-A081 919

END
DATE
FILMED
4-80
DTIC



2

LEVEL

1842 EEG/EETS TR 80-6

ADA081919

AFCC TECHNICAL REPORT

DTIC
ELECTE
MAR 14 1980
C

PACKET SWITCHING TECHNOLOGY FOR ALTERNATE
CRITICAL COMMUNICATIONS NETWORK (ACCN)

This document has been approved
for public release and sale; its
distribution is unlimited.

DATA COMMUNICATIONS SYSTEMS BRANCH
1842nd Electronics Engineering Group (AFCC)
Scott Air Force Base, Illinois 62225

15 February 1980

80 3 7 045

DDC FILE COPY

1842 ELECTRONICS ENGINEERING GROUP

MISSION

The 1842 Electronics Engineering Group (EEG) has the mission to provide communications-electronics-meteorological (CEM) systems engineering and consultive engineering support for AFCC. In this respect, 1842 EEG responsibilities include: Develop engineering and installation standards for use in planning, programming, procuring, engineering, installing and testing CEM systems, facilities and equipment; performing systems engineering of CEM requirements that must operate as a system or in a system environment; operating a specialized Digital Network System Facility to analyze and evaluate new digital technology for application to the Defense Communications System (DCS) and other special purpose systems; operating a facility to prototype systems and equipment configurations to check out and validate engineering-installation standards and new installation techniques; providing consultive CEM engineering assistance to HQ AFCC, AFCC Areas, MAJCOMS, DOD and other government agencies.

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
14 1842 EEG/EETS — TR-80-6		N/A
4. TITLE (and Subtitle)		5. TYPE OF REPORT & PERIOD COVERED
6 Packet Switching Technology for Alternate Critical Communications Network (ACCN)		N/A
7. AUTHOR		8. CONTRACT OR GRANT NUMBER(s)
10 Henry/Kin Darrell G. Wallace		N/A
9. PERFORMING ORGANIZATION NAME AND ADDRESS		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
1842 EEG/EETSA Scott AFB IL 62225		12/23/80
11. CONTROLLING OFFICE NAME AND ADDRESS		12. REPORT DATE
1842 EEG/EETS Scott AFB IL 62225		Feb 80
13. NUMBER OF PAGES		15. SECURITY CLASS. (of this report)
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		Unclassified
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE
16. DISTRIBUTION STATEMENT (of this Report)		
Approved for public release. Distribution unlimited.		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		
N/A		
18. SUPPLEMENTARY NOTES		
N/A		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number)		
Switching, packets, packet switching, ACCN		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number)		
<p>The ACCN is in the process of modernizing their system so that it can provide a fall-back capability sufficient to sustain combat operations in the critical period just prior to and after D day. This report provides generalized tutorial information to allow ACCN personnel to better assess the best switching method to employ, whether it be Packet Switching as discussed in this report or one of the other switching techniques.</p>		

409646

JEC

APPROVAL PAGE

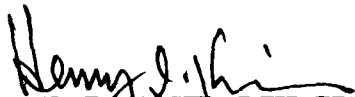
This report has been reviewed and is approved for publication and distribution.



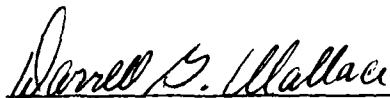
ZYGMUND J. BARA
1842 EEG/EET
Chief, Telecommunications Systems Engineering Division



C. ROY WALDRON
1842 EEG/EETS
Chief, Data Communications Systems Branch



HENRY I. KIN
1842 EEG/EETSA
Electronics Engineer, Coauthor



DARRELL G. WALLACE
1842 EEG/EETSA
Electronics Engineer, Coauthor

TABLE OF CONTENTS

<u>Paragraph</u>		<u>Page</u>
1.0	INTRODUCTION	1
2.0	ACCN CONNECTIVITY	1
2.1	ACCN - Interbase Connectivity	1
2.2	ACCN - Satellite Terminals	4
3.0	PACKET SWITCHING TECHNOLOGY	4
4.0	NETWORK DESIGN RECOMMENDATIONS	5
4.1	AMPE and Subnet Design	5
4.2	Operational Program Design and Auxiliary Software	6
5.0	ACCN PACKET - NETWORK INTERCONNECTION	8
5.1	Typical Network	8
5.2	Network Sharing	8
5.3	Network Interconnection	9
5.4	Internetwork Services	9
5.5	Network Protocolling	9
5.6	Generic Protocol Layering Complications	11
6.0	UNRESOLVED QUESTIONS	11
7.0	CONCLUSIONS	11

LIST OF FIGURES

<u>Figure No.</u>	<u>Title</u>	<u>Page</u>
1	ACCN Switching Network	2
1A	ACCN Packet-Switching Interconnection Scheme (Typical)	3
2	Levels of Protocol Interaction	12
3	Protocol Layering with Internetwork Datagram	13
4	Host Protocol Translation Gateway	13

LIST OF TABLES

<u>Table No.</u>	<u>Heading</u>	<u>Page</u>
1	Generic Protocol Layers	10

Accession For	
NTIS GRA&I	<input checked="" type="checkbox"/>
DDC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	<input type="checkbox"/>
By _____	
Distribution/_____	
Availability Codes	
Dist	Avail and/or special
A	

PACKET SWITCHING TECHNOLOGY FOR ALTERNATE CRITICAL COMMUNICATIONS NETWORK (ACCN)

SUMMARY

This report provides technical information on packet switching operation for use by Alternate Critical Communications Network (ACCN) personnel. This report does not intend to imply that packet switching meets their needs better than circuit switching, message switching, or a hybrid switching network. It is strictly meant to provide tutorial system information on packet switching.

1.0 INTRODUCTION.

1.1 The Alternate Critical Communications Network (ACCN) is an element of a broader USAFE communications survivability program. This program attempts to achieve advanced survivability of USAFE's critical combat support communications via a highly survivable limited capacity voice and record communications capability for essential combat support users. The USAFE Alternate Critical Communications Network is intended for use as a full-time system that is capable of providing a backup capability sufficient to sustain combat operations in the critical period just prior to and after D-day.

1.2 The reader is cautioned that in this report we are discussing a unified message and packet switch network (Figure 1). This combined message and packet switch network is obtained by adding a front-end processor with packet switching software at each AF AMPE or other message switch site. This processor will have the capability to translate the store and forward mode of the existing AF AMPE or message switch to the packet switching mode needed for the communications media.

2.0 ACCN Connectivity. Following is the brief discussion of the various elements of the ACCN as proposed by USAFE/DC Survivability Program for the USAFE C³P² for FY 82.

2.1 ACCN - Interbase Connectivity.

2.1.1 This element of the ACCN is shown in Figure 1. It provides alternate (commercial leased and/or allied military) circuit connectivity and nodal switching. Survivability is enhanced through the use of a parallel independent switching network in combination and coordination with the European DCS. It also provides for dedicated leased circuits to reallocate existing Command and Control (C²) record communications terminals in USAFE's semi-hardened combat operation centers (COC's) to ACCN nodal switches. Nodal switching will be provided by the programmed automated message processing systems at Sembach Allied Tactical Operations Center (ATOC) and Ramstein AB and two additional ACCN message processors at the USAFE NATO Operations Support Cell (NOSC), Kalkar Germany (GE) and a suitable location in the United Kingdom (UK). USAFE main operating bases (MOB's) and collocated operating bases (COB's) in the 4th Allied Tactical Air Force (ATAF) area will be tied to Sembach. MOB's, COB's and standby bases (SB's) in the UK will be tied to the UK Switch. COB's, USAFE Tactical Air Control System (TACS) and selected NATO users will be tied to Ramstein. Message processing systems at Sembach, Ramstein, NOSC and UK locations will be

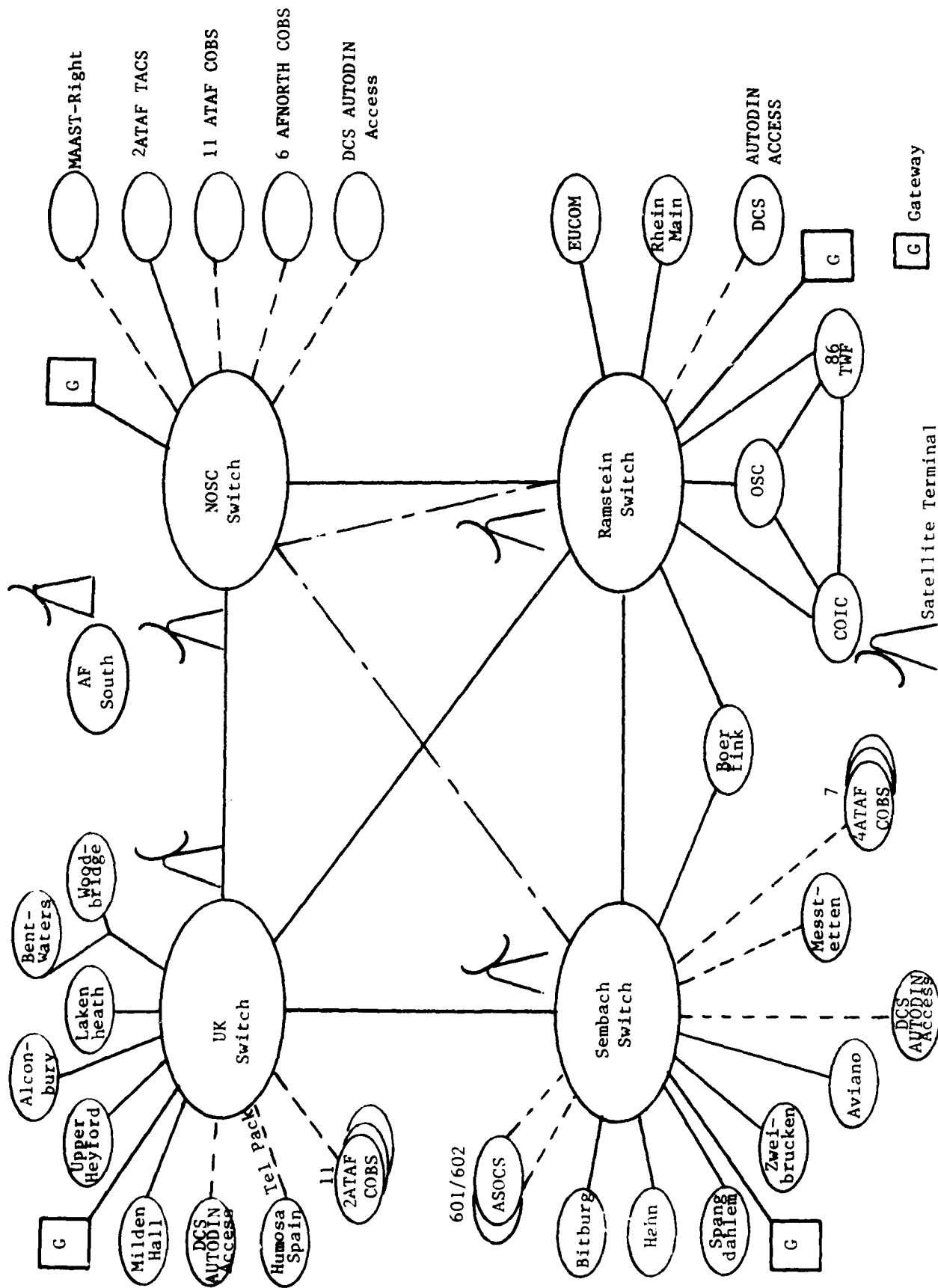


Figure 1. ACCN Switching Network

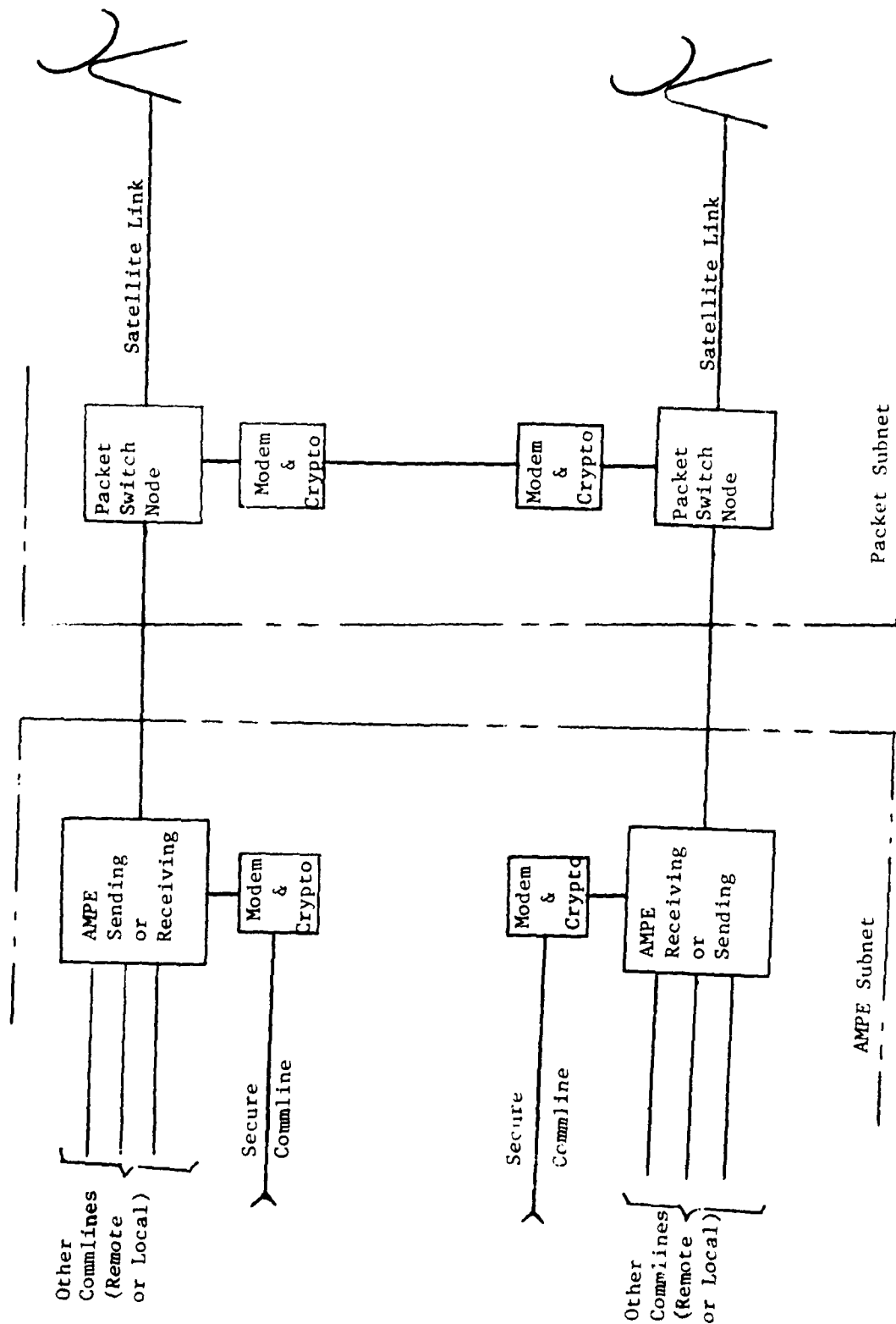


Figure 1A. ACGN Packet-Switching Interconnection Scheme (Typical)

internetted and connected to the DCS. ACCN will share dedicated leased circuits to European Satellite and submarine cable gateways for alternate long haul connectivity to CONUS, UK and NATO southern flank locations. Also the use of dedicated leased alternate routes for critical special purpose data circuits supporting USAFE WWMCCS and intelligence requirements will be allotted for this program.

2.1.2 The ACCN Switching approach is a first step toward implementation of the DCA plan to remove switching functions from vulnerable backbone nodes and collocate them with user communities. Distributed ACCN switches working in conjunction with existing DCS switches will greatly enhance survivability.

2.2 ACCN - Satellite Terminals.

2.2.1 The USAFE ACCN relies on redundant and diverse communications media to achieve survivability. Because of the European/NATO geographical and political constraints, the ACCN is divided into three principal regions; the United Kingdom, Central Europe (North of the Alps) and the Southern Flank (Italy, Greece, Turkey and Mediterranean). Reliable commercial leased communications are available to satisfy ACCN connectivity and survivability requirements in the UK and Central Regions. For the Southern Flank region the SATCOM is the ideal media for ACCN requirements.

3.0 PACKET SWITCHING TECHNOLOGY.

3.1 The packet - switching technique provides an efficient mixture of many users and many data rates on a single channel. Terminals of all types and speeds, from the lowest speed interactive terminals to the highest speed batch devices are enabled by the packet switching methodology to access to the network. This packet switch network allows users to access through interconnection with computers on other networks and in other countries. The Packet Switch Nodes (PSN) format the data that is to be sent into "packets" with fixed length format headers. Wideband communication links interconnect the PSN's the network being designed so that if one of the lines is busy or fails there is always an alternate line. These PSN's dynamically determine the best routing for their "packets", and the message packets are passed very quickly from one PSN to another. The packet is never put in secondary storage, as in message-switching systems. Most of the current networks use 50 kb/s lines, and packets traverse the switching network in less than 100ms of transition time. The transmission between PSN's can be made virtually error free with highpower error detecting codes and correction by retransmission. Computers using any different code can be attached to the network via its interface message processing devices. Any data can be sent, from very low speed to the highest speed of the network due to the effective multiplexing achieved by packetizing the data streams.

3.2 A packet-switching network, the node switches all have a complete knowledge of the status of the network. In the event of status change; for example, if a node switch fails, a line (channel) fails, or an area becomes congested, control messages indicating this fact pass throughout the entire network, and the network status tables in each node are updated. These status tables enable each node to route all packets to a destination marked in their header by the most efficient routing (choice of alternate lines). When a node becomes

temporarily congested, it sends a "shut-up" message to its neighbors who temporarily route their packets so as to avoid the congestion. This technique is known as Automatic Adaptive routing.

3.3 This paper discusses the design requirements of the ACCN packet-switching subnet and attempts to describe the hardware, the software, and the predicted performance of the Automated Message Processing Exchange (AMPE) used in the USAFE installations. The issues of end-to-end protocol and network utilization are barely touched upon. The US Department of Defense policy is to employ common-user networks to the maximum extent possible. AUTODIN II is being developed in order to stop the proliferation of specialized data networks for specific applications such as logistics and other bulk compiled transactions. However, interoperability requirements become more severe in a NATO environment. The NATO Integrated Communications system does not at present interoperate with the many national defense communications systems. Currently, NATO is planning for interoperability of national defense communications networks under a high priority task force.

4.0 NETWORK DESIGN RECOMMENDATIONS.

4.1 AMPE and Subnet Design. The design of the ACCN packet-switching network is discussed in two parts. In the first part we will cover requirements for development of relations between the AF AMPES's and the PS subnet, and in the second part we will discuss the design of the subnet itself.

4.1.1 During the system design planning stage a series of questions about the relationship between the AF AMPES subnet and PS subnet (Figure 1A) should have their answers (or at least their impact) considered: What tasks shall be performed by each AF AMPE and Packet Switch Node (PSN)? What constraints shall each place on the other? What dependence shall the subnet have on the AF AMPES's? In considering these questions, we are guided by the following principles:

- o The packet switching network should function as a communication system whose essential task is to transfer data reliably and efficiently from a source location to a specified destination. Data transmission should be sufficiently reliable and error free to obviate the need for special precautions (such as storage for retransmission) on the part of the PSN;

- o The average transit time through the packet switch network should be less than two seconds to provide for convenient interactive use of remote processors:

- o The packet switch network operation should be completely autonomous. The packet switch network must function as a temporary store and forward system for packets. The packet switch must continue to operate whether the AF AMPE is functioning properly or not and must not depend upon the AF AMPE for buffer storage or other logical assistance such as program reloading. The AF AMPE must not in any way be able to change the logical characteristics of the packet switch network; this restriction avoids the mischievous or inadvertent modification of the communications system by an individual AF AMPE user:

- o Establishment of end-to-end protocol and the enormous problem of planning to communicate between different processors should be an issue separated from the PS network design.

4.1.2 A major hazard in a PS network is congestion, which can arise either due to system failures or to peak traffic flow. To solve this problem, PS network designers have developed throttling schemes which limit the flow of messages to a given destination when congestion begins to occur, or when messages are simply not getting through. When a path becomes unblocked, the PS network notifies the source by sending it a special control message defined by the network access protocol which allows transmission to resume. When giving the PS network a message, the AF AMPE specifies the destination subscriber in the header of the message. The packet switch then handles the route selection, delivery, and notification of receipt.

4.1.3 AF AMPE's communicate with each other via a sequence of messages. A PSN takes in a message from its AF AMPE in segments, forms these segments into packets (whose maximum size is approximately 1000 to 5000 bits), and ships the packets separately into the network. The destination PSN reassembles the packets and delivers them in sequence to the receiving AF AMPE, who obtains them as a single unit.

4.1.4 Each packet is individually routed from PSN-to-PSN through the network toward the destination. At each PSN along the way, the transmitting hardware generates framing characters and parity check digits that are added to the packet and used for error detection by the receiving hardware of the next PSN. Each PSN stores the packet until a positive acknowledge is returned from the succeeding PSN. The source PSN stores packets until an acknowledgement is received from the destination PSN. However, an AMPE is always free to refuse a packet by simply not returning a positive acknowledgement. It may do this for any of several reasons: the packet may have been received in error, the PSN may be busy, the PSN buffer storage may be temporarily full, etc. At the transmitting PSN, such discard of a packet is detected and retransmitted as a new packet according to the line protocol rules. Duplicate packets may be generated when acknowledgements are lost, etc. The destination PSN sorts out any resulting duplication by using a message number and the packet number in the header. The packets of a message arrive at the destination PSN, possibly out of order, where they are reassembled. The header is then stripped off each packet and a header, identifying the source Host and the path, followed by the reassembled message is then delivered to the destination subscriber as a single unit.

4.2 Operational Program Design and Auxiliary Software. Implementation of a packet switch network requires the development of a sophisticated operational computer program and several auxiliary programs for hardware tests, program construction, and debugging. This section of the paper discusses briefly the design of the operational program and touches on the description of the auxiliary software.

4.2.1 The principal function of the operational program is the processing of packets. This processing includes segmentation of AF AMPE messages into packets for routing and transmission, building of headers, temporary storage of packets, receiving, routing and transmitting of packets, and handling protocols. The program also monitors network status, gathers statistics, and performs on-line testing. This real-time program is an efficient, interrupt-driven, involute program.

4.2.2 The major system data structures, usually, consist of buffers and tables. A packet, once stored in a buffer, is never moved. After a packet has been successfully passed along to its AF AMPE or to another PSN, its buffer is cleared and returned to the free list. The buffer space is partitioned in such a way that each process is always guaranteed some buffers. For the sake of program speed and simplicity, no attempt should be made to retrieve the space wasted by partially filled buffers.

4.2.3 Buffers in use are either dedicated to an incoming or outgoing packet, chained on a queue awaiting processing by the program, or being processed. Occasionally, a buffer may be simultaneously found on two queues; this situation can occur when a packet is waiting on one queue to be forwarded and for another to be acknowledged.

4.2.4 Software should be modularized to simplify design and maintenance. Most software modules will operate under the control of a real-time executive program which manages buffer space, schedules subordinate programs as necessary, handles input/output, and permits inter-task communication. In systems which handle multiple levels of security, a portion of the executive should be written to ensure the rules of security are not broken by untrusted software modules. Other modules will perform the actual communications tasks. Line protocol routines will handle communications at the line level to control modems, detect line errors, and to communicate with other devices. Recent technological advances have permitted this function to be handled by microprocessors on the periphery of the main processor thus giving the main processor more time for other tasks. Other routines will include header generation and addressing, routing control, congestion control, and end-to-end and local protocols.

4.2.5 The control structure and partition of responsibility among various program functions usually achieve the following timing goals:

- o No program stops or delays the system while waiting for an event.
- o The program gracefully adjusts to the situation where the machine becomes congested due to computation limitations.
- o Necessary periodic processes (in the time-out routine) are always permitted to run, and do not interfere with input-output processes.

4.2.6 The operational program requires not only unusual techniques but also extra software tools. The development of the AF AMPE integrated packet switching system (Figure 1) requires the following kinds of supporting software:

- o Programs to test the hardware.
- o Software Certification tools
- o Tools to help debug the system.
- o An interface simulator.
- o Assemblers and/or compilers

4.2.7 Except for possibly the interface simulator, all of the above support software is available from many sources "off-the-shelf". The simulator may require development; but should present few problems.

5.0 ACCN PACKET-NETWORK INTERCONNECTION.

5.1 Typical Network. A typical ACCN Packet-network should have provisions for security, precedence control, and establishment of close communities of interest and should sustain a high level of reliability, survivability and message throughput (see Figure 1A). The problems confronting the ACCN record network introduce a wide range of technical, legal, and political issues associated with the interconnection of packet-switched data communication networks. The technical issues generally revolve around mechanisms for achieving interconnection and their performance. How can networks be interconnected so that packets can flow in a controllable way from one net to another (USAFE/NATO/CONUS)? Should all computer systems on all nets be able to communicate with each other? How can this be achieved? What kind of performance can be achieved with a set of interconnected networks of widely varying internal design and operating characteristics? How are terminals to be given access to resources in the other networks? What protocols are required to achieve this? Should the protocols of one net be translated into those of another, or should common protocols be defined? What kind of communication protocol standards are needed to support efficient and useful interconnection? Who should take responsibility for setting standards?

5.2 Network Sharing. More networks today are beginning to share resources to increase survivability, to obtain a centralized service, to get otherwise unavailable automated services, or to obtain a cost savings. How can two networks A and B, which share resources, be arranged so that a subscriber on network A cannot overload network B to the point that subscribers of network B are denied service? Denial of service can be controlled by use of protocols, priorities, and network hierarchy which throttle the data exchanges. Service denial must be given serious consideration in any system design.

5.2.1 The legal and political issues are at least as complex as the technical ones. Can private networks interconnect to each other or must they do so through the mediation of a public network? How is privacy to be protected? Should there be control over the kinds of data which moves from one net to another? Are there international agreements and connections which might be affected by international connection of data networks? How can faults and errors be diagnosed in a multinet environment? Who should be responsible for correcting such faults? Who should be responsible for maintaining the gateways which connect nets together? This paper does not attempt to answer all of these questions, but we deal with many of them in the objectives of the requirements.

5.2.2. A consequence of the wide range of technologies which are optimum for specific packet-switching applications is that many different networks, both USAFE and NATO, may co-exist. A network interconnection strategy, if properly designed, will permit interfacing networks to be optimized without sacrificing the possibility of providing effective internetwork services. Two unique developments can be expected. First, organizations which are dispersed geographically, nationally, or internationally, will want to interconnect their networks both to share centralized resources and to effect intra-organization electronic message and other automated office services. Second, there will be an increasing interest

in interorganization interconnections to allow automated procurement and security transaction services, those applied to interorganization affairs.

5.3 Network Interconnection. The ultimate choice of a network interconnection strategy is usually affected by the types of user services which must be supported. Most of the currently prevalent computer-communication services fall into four categories:

- o Terminal access to time-shared host computer
- o Remote job entry (RJE) services
- o Bulk data transfer
- o Transaction processing

The time-sharing and transaction services typically demand short network and host response times but modest bandwidth. The RJE and file transfer services more often require high amounts of data transfer, but can tolerate longer delay. Packet switching techniques permit both types of service to be supported with common network resources. Bulk data transfer requires increasingly higher throughput rates if delivery delays are to be kept constant as the amount of data to be transferred increases. As distributed operating systems become more prevalent, an increased need for end-to-end transaction services will be dictated.

5.4 Internetwork Services. The problem of achieving a useful set of internetwork services might be approached in several ways, as follows:

5.4.1 Require all networks to implement the entire range of desired services (i.e. datagram, broadcast, real-time, etc.) and then attempt to support these services across the gateways between the networks.

5.4.2 Require all networks to implement only the most basic services across gateways and rely on the subscriber to implement all other services end-to-end.

5.4.3 Allow the subscriber to identify the services (common mode of usage) it desires and provide error indications if the network involved, or the gateway between them, cannot provide the desired services.

5.4.4 Allow the subscriber to specify the internetwork route to be followed for dual homing and depend on the subscriber to decide which concatenation of services are appropriate and what end-to-end protocols are needed to achieve the preferred class of services.

5.4.5 Provide one set of services for local use within each network and another, possibly different set, for internetwork use.

Although the five choices above are by no means exhaustive, these are leading steps for initial network analysis and evaluation.

5.5 Network Protocolling. A useful concept of network protocolling must be designed. Table I offers a very generic view of a typical protocol hierarchy in a packet switching computer network, including layers usually found outside of the communication network itself to provide services in a single network and to compare the capabilities of different network.

TABLE I
GENERIC PROTOCOL LAYERS

PROTOCOL LAYER	FUNCTIONS
6. APPLICATION	FUNDS TRANSFER, INFORMATION RETRIEVAL, ELECTRONIC MAIL TEXT EDITING . . .
5. UTILITY	FILE TRANSFER, VIRTUAL TERMINAL SUPPORT
4. END/END SUBSCRIBER	INTERPROCESS COMMUNICATION (E.G. VIRTUAL CIRCUIT, DATAGRAM, REAL-TIME, BROADCAST)
3. NETWORK ACCESS	NETWORK ACCESS SERVICES (E.G. VIRTUAL CIRCUIT, DATAGRAM . . .)
2. INTRANET, END-TO-END	FLOW CONTROL, SEQUENCING
1. INTRANET, NODE-TO-NODE	CONGESTION CONTROL ROUTING
0. LINK CONTROL	ERROR HANDLING, LINK FLOW CONTROL

5.6 Generic Protocol Layering Complications. There are several complications to the use of generic protocol layering to new design network interconnection issues. Chief among these is that networks do not all contain the same elements of generic hierarchy. A second complication is that some networks implement service functions at different protocol layers. Finally, the hierarchical ordering of functions is not always the same in all networks. The ascending protocol hierarchy shown in Table I is a conventional depiction of the seven level global network architecture similar to that recommended by the International Organization for Standards (ISO).

6.0 UNRESOLVED QUESTIONS.

6.1 To date there are many unresolved questions; primarily these questions have a technical, policy administrative, regulatory, or operational aspect, or a combination of these. One example of this is the question of the procedures to be used for internet routing.

6.2 Also, there are technical questions on what is feasible in view of the technologies used in the subnets; there are policy questions on when a third country routing might be allowed; there are economic considerations on how much it would cost to do the necessary protocol translation to route through third countries, and on what charges the connecting transmit network might make; there may be regulatory questions on which classes of data may flow through specific countries (related to the transnational data flow regulations); and there may be operational questions on whether in the event of failure in dynamic rerouting, reestablishment could take place with sufficient rapidity.

7.0 CONCLUSIONS.

7.1 In view of all the unresolved questions discussed in this paper, most of the conclusions can be drawn in this presentation must be considered as tentative. From the early part of the paper, we have discussed that it is essential that techniques be developed for connecting ACCN AMPE Networks. It should be understood, that no single set of techniques will fit all applications as shown in Figure 1. The ACCN switching network as shown in Figure 1 will require a more complex network if tied to other communication systems. The fundamental role of the gateway is to terminate the internal protocols of each network (See Figures 3 and 4) to which it is connected while, at the same time, providing a common connection across which data from one network can pass into another. The term "gateway" need not imply a monolithic device which joins a pair of networks. The gateway may be only software in a pair of packet switches in different networks, or it may be made of two parts, one in each network (a sort of "gateway half" $\frac{1}{2}G$). In the latter case, the two devices might be devices separate and distinct from the network packet switches or might be integrated with them. Furthermore, a gateway might interconnect more than two networks. It is worth pointing out, that the " $\frac{1}{2}G$ " gateway concept is highly attractive from both a technical and administrative point of view. Technically, each half could terminate certain levels of protocol of the net to which it is attached. Administratively each half could be the responsibility of the network to which it belongs. Then the only matters for jurisdictional negotiation are the physical medium by which the half-gateways exchange data, and the format and protocol of the exchange.

7.2 The basic internet datagram service could be used to support transaction protocols (See Figure 3) or real-time protocols (RTP) such as packet-voice

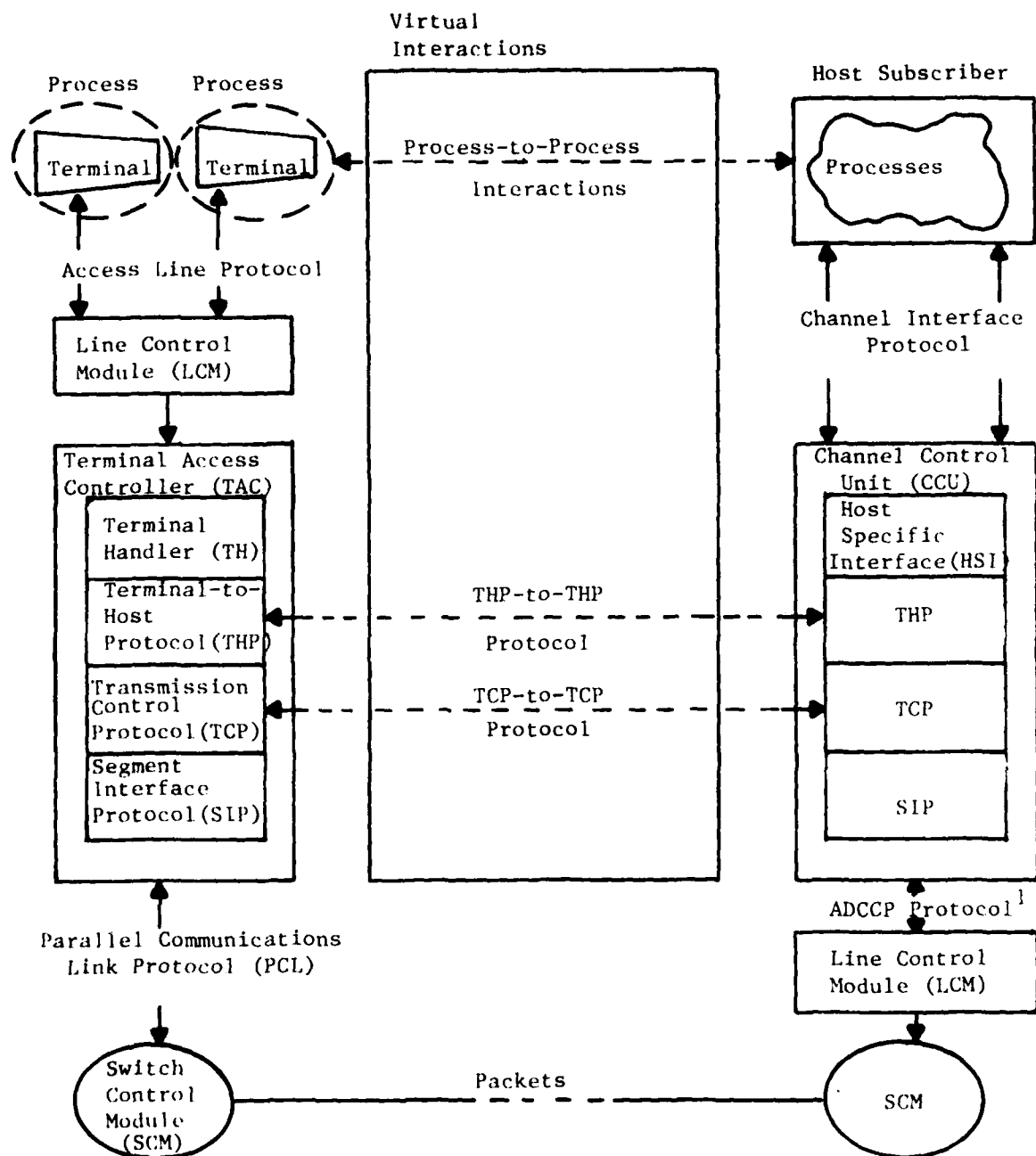


Figure 2. Levels of Protocol Interaction
Source: AUTODIN II Design Plan Vol VI, Appendix D

¹ADCCP - Advanced Data Communications Control Procedures

UTILITY	FTP	VIP	RTP	VP
End/End Subscriber	End/End Virtual Circuit		End/End Datagram	
Internet Access	Internet Datagram			
Network Access	Network Specific			
Intranet, End-End	Network Specific			
Intranet Node-Node	Network Specific			
Link Control	Network Specific			

Figure 3. Protocol Layering with Internetwork Datagram

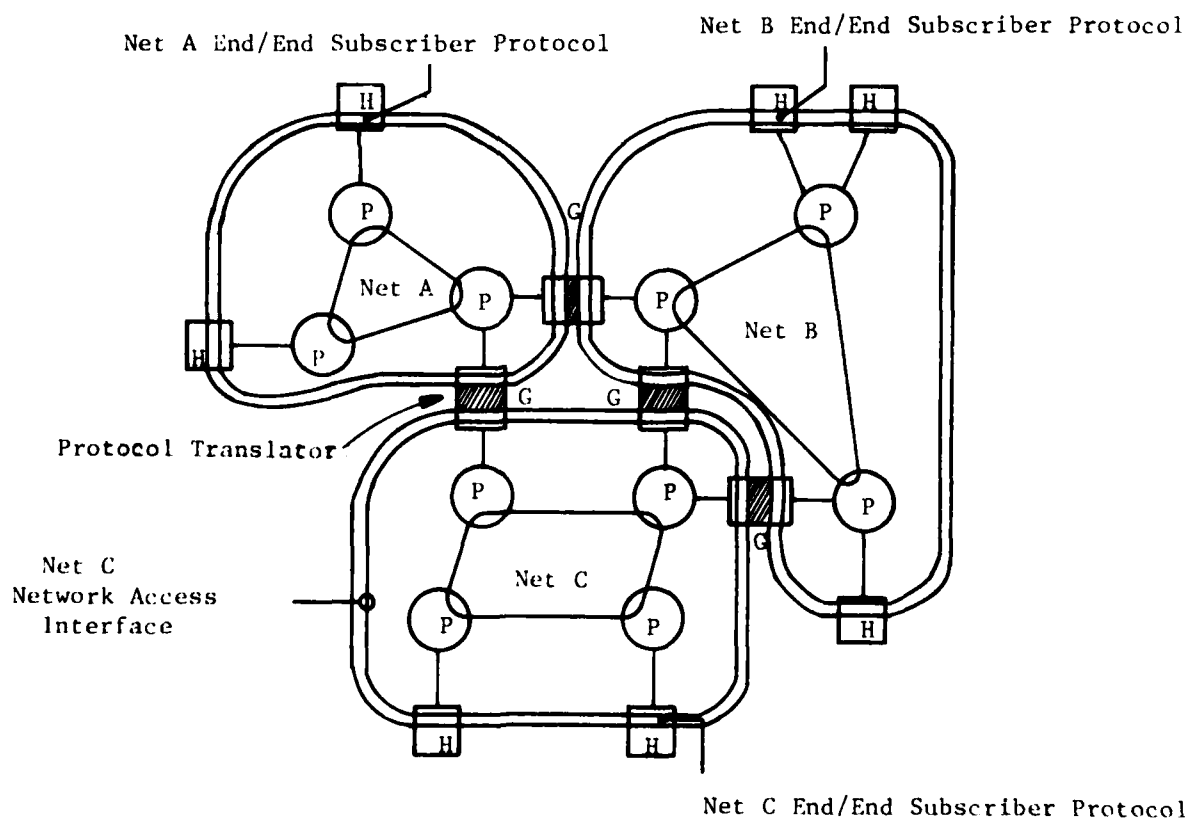


Figure 4. Host Protocol Translation Gateway

protocols (PVP) which do not require guaranteed or sequenced data delivery. Application such as virtual terminal protocols (VTP) could be built above a reliable, point-to-point, end-to-end service which is itself built atop internet datagrams. Under this strategy, the basic gateway functions are the encapsulation and decapsulation of datagrams, mapping of internet source/destination addresses into local network addresses and datagram routing. Gateways need not contain higher level protocols if it is assumed that protocols above the internet datagram layer are held in common by the communicating hosts. The basic packet carrying service of one network is being translated into the next network's packet carrying service (See Figure 4). This concept could be extended further. For example, if two networks have a virtual circuit concept, (See Figure 2), one implemented within the subnetwork and the other through common Host/Host protocols, it might be possible, at the gateway between the nets, to map one network's virtual circuit into the other's. This same idea could be applied to the higher level protocol mapping as well; for instance, the virtual terminal protocol for one network might be transformed into that of another.

7.3 The services which normally have to be supported are terminal access, bulk transfer, remote job entry, and transaction processing. The quality and facilities of the services required will be very dependent on the applications. The connections between networks can be made at the level of the packet switches or AF AMPE, and can be on a datagram or virtual call basis. Connections at the packet-switch level requires broadly similar network access procedures, or complex protocol transformation at the gateways between the networks. If the network protocols are different, interconnection can be most easily achieved if done at the host level. The higher levels of service can be mapped at service centers, which need not be collocated with the gateways - but differing philosophies of network services can generate difficulties in the mapping procedures. Alternatively, subscribers can implement common higher level protocols if these can be agreed upon. The principal problems in connecting networks are much the same as those in the design of the individual networks of heterogeneous systems - but the lack of a single controlling authority can make the multinet design problem more difficult to solve. It is essential to resolve the usual problems of flow control, congestion control, routing, addressing, fault recovery, flexibility, protocol standards, and economy. At the higher levels of protocol, much more standardization is required before one has really satisfactory long term solutions. Many technical solutions to the problems of the connection of networks are discussed in this paper. Their applicability in view of ACCN utilization shall be analyzed under different technical, economic, and policy constraints imposed in different countries under consideration.

DEFINITION OF TERMS

It is important for the reader not to make any priority assumptions about the physical realization of the objects named or of the boundary of jurisdictions owning or managing them. For instance, a "gateway" might be implemented to share the hardware of a packet switch and be owned by a packet-switching service carrier; alternatively it might be embedded in an AMPE which subscribes to service on two or more computer networks. We are assigning names to groups of functions which may or may not be realized as physically distinct entities.

AMPE: A store and forward message processing system designed to serve as base level telecommunications centers. Message transmission and reception is provided with AUTODIN via remote terminals, computer interfaces and over-the-counter service. The AF AMPE system is presently available in a two or three processor configuration. Both configurations provide identical system functions; however, the three processor systems have greater message handling capability.

PACKET: A packet of information is a finite sequence of bits, divided into a control header part and data part. The header will contain enough information for the packet to be routed to its destination. There will usually be some checks on each such packet, so that any switch through which the packet passes may exercise error control. Packets are generally associated with internal packet network operation and are not necessarily visible to Host computers attached to the network.

DATAGRAM: A finite length packet of data together with destination Host address information, and source address which can be exchanged in its entirety between hosts, independent of all other datagrams sent through a packet switch network. Typically, the maximum lengths of a datagram lies between 1000 and 8000 bits.

GATEWAY: The collection of hardware and software which utilizes the basic packet-switching service to support end-to-end interprocess communication and user services. It is used to interface dissimilar networks.

PACKET SWITCH (PS): The collection of hardware and software resources which implements all intranetwork procedures such as routing, resource allocation, and error control and provides access to network packet switching services through a host/network interface.

PROTOCOL: A set of communication conventions, including formats and procedures which allow two or more end points to communicate. The end points may be packet-switches, hosts, terminals, people, file systems, etc.

TERMINAL: A collection of hardware and possibly software which may be as simple as a character-mode teletype or as complex as full scale computer system. As terminal increase in capacity, the distinction between "host" and "terminal" may become a matter of nomenclature without technical substance.

AUTODIN II: A DOD common user packet switching based system designed to provide data communications service for interactive timesharing and transaction-oriented systems requiring rapid response between terminals and computers, and computer-to-computer data transfers requiring high transmission capacity.

We have introduced these definitions as noncontroversial as possible. In the definition of PACKET-SWITCH, we alluded to a host/network interface. It would not be assumed that subscriber services are limited to those offered through the AMPE/Packet switch-interface. The packet switching carrier might also offer host-based services and terminal access mechanisms as additional subscriber services.

REFERENCES

1. The USAFE/DCRC Alternate Critical Communications Network (ACCN) (Handout Notes)
2. Trip Report - Visit to AFCC, AFCCPC and HQ USAF, 26 - 30 Nov 79, by Larry A. Robinson, Major, USAF
3. L. G. Roberts, "Telenet: Principles and Practice" in Proc. Eur. Computing Conf. Communication Networks. London, England pp 315 - 329, 1975.
4. V. G. Cerf and R.E. Kahn, "A Protocol for Packet Network Interconnection". IEEE Trans. Commun. Technol. 1974
5. L. Pouzin, "Virtual Circuits vs. Datagrams - Technical and Political Problems", in Proc. Nat. Computer Conf., AFIPS Press, 1976.
6. A. S. Chandler, "Network Independent High Level Protocols", in Proc. Eur. Computing Conf. Communication Networks, London England, 1975.
7. P. Curran, "Design of a Gateway to Interconnect the DATAPAC and TRANSPAC Packet Switching Networks", Computer Communication Networks Group, E-Report E-67, University of Waterloo, Canada, 1977.
8. P. Baran "On Distributed Communications Networks" IEEE Trans. on Comm. Systems, 1964.
9. AUTODIN II Design Plan Vol VI, Appendix D.

DISTRIBUTION PAGE

AFCC/CD	3
1842 EEG/CC	1
1842 EEG/EEIS	2
1842 EEG/EETS	2
NCA/EIE	1
SCA/EIE	1
PCA/EIE	1
AFCC/CS	1
AFCC/EP	1
Defense Technical Information Center	2
HQ USAFE/DCRC ATTN Maj Robinson Ramstein AB, GE	2